Computers in Biology and Medicine 136 (2021) 104707

Contents lists available at ScienceDirect

Computers in Biology and Medicine

journal homepage: www.elsevier.com/locate/compbiomed

Securing Bio-Cyber Interface for the Internet of Bio-Nano Things using Particle Swarm Optimization and Artificial Neural Networks based parameter profiling

Sidra Zafar [a,**], Mohsin Nazir [a], Aneeqa Sabah [b], Anca Delia Jurcut [c,*]

[a] Department of Computer Science, Lahore College for Women University, Lahore, 54000, Punjab, Pakistan
[b] Department of Physics, Lahore College for Women University, Lahore, 54000, Punjab, Pakistan
[c] School of Computer Science, University College Dublin, Dublin, Dublin 4, Ireland

ARTICLE INFO

Keywords:
Bio-cyber interface
Internet of bio-nano things
Particle swarm optimization
Artificial neural network
Parameter profiling

ABSTRACT

Internet of bio-nano things (IoBNT) is a novel communication paradigm where tiny, biocompatible and non-intrusive devices collect and sense biological signals from the environment and send them to data centers for processing through the internet. The concept of the IoBNT has stemmed from the combination of synthetic biology and nanotechnology tools which enable the fabrication of biological computing devices called Bio-nano things. Bio-nano things are nanoscale (1–100 nm) devices that are ideal for in vivo applications, where non-intrusive devices can reach hard-to-access areas of the human body (such as deep inside the tissue) to collect biological information. Bio-nano things work collaboratively in the form of a network called nanonetwork. The interconnection of the biological world and the cyber world of the Internet is made possible by a powerful hybrid device called Bio Cyber Interface. Bio Cyber Interface translates biochemical signals from in-body nanonetworks into electromagnetic signals and vice versa. Bio Cyber Interface can be designed using several technologies. In this paper, we have selected bio field-effect transistor (BioFET) technology, due to its characteristics of being fast, low-cost, and simple The main concern in this work is the security of IoBNT, which must be the preliminary requirement, especially for healthcare applications of IoBNT. Once the human body is accessible through the Internet, there is always a chance that it will be done with malicious intent. To address the issue of security in IoBNT, we propose a framework that utilizes Particle Swarm Optimization (PSO) algorithm to optimize Artificial Neural Networks (ANN) and to detect anomalous activities in the IoBNT transmission. Our proposed PSO-based ANN model was tested for the simulated dataset of BioFET based Bio Cyber Interface communication features. The results show an improved accuracy of 98.9% when compared with Adam based optimization function.

1. Introduction

Internet of Bio-Nano Things (IoBNT) is an emerging ICT paradigm that defines a set of networks for communication between natural and artificial nanoscale entities like nano biosensors or genetically engineered bacteria, and Information and Communication (ICT) based applications integrated with the Internet infrastructure Akyildiz, Pierobon, Balasubramaniam and Koucheryavy [1]. IoBNT aims for connectivity and control over non-conventional domains such as the human body. The primary objective of the Internet of bio Nano Things paradigm is to detect biochemical signals from in vivo environments and forward the detected information to external networks (Internet) for analysis and processing. To this aim, various heterogeneous nano to macro-scale devices works collaboratively. The seamless integration and communication between these heterogeneous devices is the main goal in the realization of IoBNT. Several factors affect the direct communication between nano and macro scales devices such as the difference between transceiver sizes, computation capabilities, and storage capacities.

The minute size of nanodevices makes them resource-constrained and unable to communicate directly with macro-scale devices. To achieve this objective a hybrid device needs to be incorporated within IoBNT architecture that can convert biochemical signals from inbody

* Corresponding author.
** Corresponding author.
E-mail addresses: sidra.zafar@lcwu.edu.pk (S. Zafar), mohsin.nazir@lcwu.edu.pk (M. Nazir), aneeqas29@gmail.com (A. Sabah), anca.jurcut@ucd.ie (A.D. Jurcut).

https://doi.org/10.1016/j.compbiomed.2021.104707
Received 11 May 2021; Received in revised form 8 July 2021; Accepted 24 July 2021
Available online 31 July 2021

into electromagnetic signals for communication with the Internet and vice versa. This device is called the bio cyber interface which can provide a seamless interface to the biological world inside the human body and the cyber world of the Internet Akyildiz et al. [1]. The design of bio cyber interface is a major challenge in the realization of IoBNT and has attracted significant research attention. Several technologies have been investigated to perceive an operational bio cyber interface i.e., redox-based chemoelectro transconductance units Kim, Li, Kang, Kelly, Chen, Napolitano, Panzella, Shi, Yan, Wu et al. [2], FRET (Fluorescence Resonance Energy Transfer)based bio cyber interface Abd El-atty, Bidar and El-Rabaie [3], optical to chemical biological interface Grebenstein, Kirchner, Peixoto, Zimmermann, Irnstorfer, Wicke, Ahmadzadeh, Jamali, Fischer, Weigel et al. [4] and BioFET based MC-Rx Kuscu and Akan [5]. In this paper, we have selected bio field-effect transistor (BioFET) technology, due to its characteristics of being fast, low-cost, and simple Sadighbayan, Hasanzadeh and Ghafar-Zadeh [6]. The range of BioFET's bio-medical applications is extensive, such as BioFETs for detecting antigens (especially viruses) Park, Choi, Jeun, Kim, Yuk, Kim, Song, Lee and Lee [7]; Chen, Ren, Pu, Guo, Chang, Zhou, Mao, Kron and Chen [8], BioFETs for detecting biomarkers of certain diseases Salehirozveh, Dehghani, Zimmermann, Roy and Heidari [9], and BioFETs for drug screening Pham Ba, Han, Cho, Kim, Lee, Kim and Hong [10]; Pham Ba, Cho and Hong [11]. The bioFET based MC-Rx is considered as the main approach in the literature, therefore we have adopted bioFET based bio cyber interface in our study. IoBNT has many applications in the environmental, industrial, and bio-medical fields. The most promising application of IoBNT is bio-medical applications such as intra-body continuous health monitoring and theranostic systems with single molecular precision like targeted drug delivery and nano surgeries. There is an accelerated need for continuous and remote healthcare services in this era of pandemics like COVID 19 and associated social distancing regimes. The advent of IoBNT has provided an avenue for advanced and most sophisticated healthcare. The nanosize is an edge for healthcare applications, as these devices can reach hard-to-access areas (like deep inside tissue) for sensing and actuation. The idea of IoBNT seems fascinating with its plethora of applications. But, as soon as the human body is given access to be manipulated through Internet, there is always a possibility that it will be done with malicious intent. This work proposes a comprehensive security framework for bioFET based bio cyber interface of IoBNT. An Artificial Neural Network-based profiling scheme is used to differentiate between the normal and anomalous activity of bio cyber interface. PSO algorithm is used to optimize the employed ANN. The PSO algorithm utilizes an elementary theory and exhibits sustainable performance; therefore, it is a convenient method for determining the optimal weights and biases of neurons in different ANN layers, with a very high probability and convergence. The proposed security frame is trained using extensive simulations on data presenting significant attributes of bioFET based bio cyber interface. In summary, the contributions of this paper are presented below:

- Identifying and simulating the communication parameters for BioFET based bio cyber interface.
- Individuating of security concerns specific to BioFET interfaces.
- Implementation of Particle Swarm Optimizer (PSO) for Artificial Neural Network (ANN).
- To propose a security framework for bio cyber interface of IoBNT, based on ANN classification.
- Extensive simulations to gather results and evaluate the performance of the proposed framework.

The rest of the paper is organized as follows Section 2 represents the related literature in the field of bio cyber interface security, Section 3 defines the architecture of the Internet of Bio-Nano Things. Section 4 represents the working principles of BioFET based bio cyber interface and its security concerns. Section 5 presents the details of our proposed PSO based ANN model, Section 6 and 7 represents evaluation results and conclusion respectively.

2. Literature review

Securing the bio cyber interface will play a pivotal role in the greater adoption of IoBNT applications. The security in IoBNT has started getting research attention just recently. A systematic review Zafar, Nazir, Bakhshi, Khattak, Khan, Bilal, Choo, Kwak and Sabah [12] has been recently proposed that defines IoBNT and bio cyber interface security comprehensively. A privacy scheme for bio-luminescence based bio cyber interface is proposed in El-Fatyany, Wang, Abd El-atty and Khan [13]. The authors have proposed an authentication scheme to control the drug dosage in targeted drug delivery applications of IoBNT. A chaotic system is proposed using a modified logistic map, based on the command signal sent from the healthcare provider. The proposed system utilizes a BPSK modulation scheme and ZCR (Zero Crossing rate) for feature extraction. Another work in the direction of securing bio cyber interface is proposed in Bakhshi and Shahid [14]. A machine learning-based parameter profiling is done for the authentication of three types of bio cyber interfacing technologies. Redox modality, bio-luminescence, and bioFET based technologies are considered as bio cyber interfacing options. Three prominent decision tree algorithms (ID3, C 5.0, and CART) are used for parameter profiling. According to the authors, bioFET based interfacing technology has proved to be the most promising among the other two. Molecular communication (MC) is the basic building block in realizing the IoBNT paradigm. Therefore, security in this novel communication technology must be considered during the application development phase. In the direction of MC security, a comprehensive survey on security and privacy concerning layered MC architecture is presented in Loscri, Marchal, Mitton, Fortino and Vasilakos [15]. Another work Giaretta, Balasubramaniam and Conti [16] has defined two attack types (blackhole and sentry) for molecular nanonetworks. The countermeasures proposed for the two attack types comprise of two forms of decision processes, including Bayes rule and simple threshold method. Guo, Wei and Li [17] has proposed an encryption scheme for diffusion-based MC using Channel impulse response for generating cipher keys. Furthermore, Falko dressler Dressler and Kargl [18,19] and his team have coined the term "Biochemical cryptography" as novel and lightweight cryptography primitive for resource-constrained MC. Other works in MC security encompass physical layer security of MC which include secrecy capacity for MC Mucchi, Martinelli, Jayousi, Caputo and Pierobon [20]; Singh, Yadav and Mishra [21]; Sharma, Pandey, Singh and Mallik [22], eavesdropper localization in 1-D molecular channel Guo, Deng, Li, Zhao and Nallanathan [23] and authentication of nano transmitter using CIR as device fingerprint Zafar, Aman, Rahman, Alomainy and Abbasi [24].

3. Internet of Bio nano things

In this work, we consider IoBNT concerning its bio-medical applications. The realization of a holistic IoBNT paradigm involves several heterogeneous devices and communication protocols. The architecture and components of IoBNT are described below:

- Nano network: Nano network is a set of interconnected nanodevices that can perform trivial computing functionalities like sensing the environment, data storing, and actuation. The size of nanodevice is around 1–100 nm. Nanodevices that are manufactured reprogramming biological cells, bacteria and similar entities are called bio-nano things. The considered *invivo* environment for bio-nano things in this work is inside the human body. The biological nano network cannot communicate using traditional wireless and wired communication technologies due to their tiny transceiver size, constrained resources, and biological structure. Therefore, a novel communication paradigm called Molecular Communication is

utilized for communication between bio-nano things. Molecular Communication (MC) is a novel communication paradigm that utilizes molecules for the transmission and reception of messages between living entities at the nanoscale Nakano, Moore, Wei, Vasilakos and Shuai [25]. Due to the biocompatible and robust nature of MC, it has been considered as an ideal approach for communication within environments like intrabody medium Atakan, Akan and Balasubramaniam [26], where traditional wireless communications may fail Kuscu and Akan [5]. By combining the tools of nanotechnology and synthetic biology, MC has emerged as the most promising paradigm to enable nanonetworks and the Intenet of Bio-Nano Things (IoBNT). The in-body sensory data collected by the nanonetworks in the form of biochemical signals are then transmitted to the bio cyber interface for further processing.

- Bio Cyber Interface: Bio cyber interface is a hybrid on-body device that converts the biochemical signal received from inbody nanonetworks into an electrical signal to be processed by external networks (Internet). It can be thought of as an electronic tattoo or RFID tag implanted over a convenient part of the human body like wrist Akyildiz et al. [1]. Bio cyber interface is the most vital part of IoBNT and its design implementation needs particular consideration as the operation of the entire IoBNT system depends on the accurate operation of this module. A detailed description bio cyber interface is provided in Section 4.
- Gateway devices: The electrical signal generated by the bio cyber interface is received by authorized gateway devices and is relayed to a medical server through the internet. Gateway devices include advanced smartphones, tablets, and PDAs(Personal Digital Assistant).
- Medical Server: Medical server stores and analyze the information received from nanonetworks. The processed information is utilized by a healthcare provider for continuous and real-time monitoring of patients.

A schematic illustration of IoBNT architecture is presented in Fig. 1.

4. BioFET based bio cyber interface

Molecular receivers (MC-Rx), a fundamental component of IoBNT communication are employed to recognize and detect information encoded in (any) target molecules in the vicinity and transducing the same into electrical signals for further processing Kuscu and Akan [5]. The information can be encoded in form of some physical property of these molecules such as concentration/ratio/order/type, or release time. To this aim, MC-Rx architecture can be divided into two main categories (i) Biological MC-Rx architectures and (ii) Nanomaterials based artificial MC-Rx. Synthetic biology has made it possible to modify natural gene circuits of living organisms and engineer biological nanonetworks inside them. Biological MC-Rx architectures such as synthetic gene circuits of engineered bacteria are biocompatible and thus are ideal for *in-vivo* applications such as targeted drug delivery, monitoring an organ of human beings or animals, and immune system support. A detailed review of existing biological MC-Rx architectures has been presented in Kuscu, Dinc, Bilgin, Ramezani and Akan [27]. The review has also highlighted some drawbacks of using completely biological architectures such as their restriction to be being used in *in-vivo* applications only, the low computational power of biological architectures slows down the information processing speed. Moreover, these devices cannot be integrated with an interface for macro-level networks such as the Internet, which is a major challenge for realizing IoBNT and its applications. Nanomaterials based artificial architectures is another option for MC-Rx that provides *in-situ* electrical biosensing options Kuscu and Akan [28]. Recent advances in nanotechnology have led to the design of novel architectures of MC-Rx using nanomaterials such as Nanowires (NW), graphene and organic polymers for electrical biosensing Shan, Li, Chu, Xu, Jin, Wang, Ma, Fang, Wei and Wang [29], Xu, Zhan, Man, Jiang, Yue, Gao, Guo, Liu, Li, Wang et al. [30], Kim, Song, Jin, Park, Lee, Lee, Park and Hong [31]. In this direction, MC-Rx based on the principles of bioFETs (Field Effect Transistors) is considered as a main approach literature Garralda, Llatser, Cabellos-Aparicio, Alarcón and Pierobon [32], Farsad, Eckford and Hiyama [33], which is capable of providing *in-situ*, label-free and continuous sensing of molecules as a stand-alone device Kuscu et al. [27]. The operation principles of bioFETs are similar to conventional FETs.The conventional FETs consist of three electrodes (i) source electrode, (ii) drain electrode, and (iii) gate electrode. In conventional FETs, the current flows from the source electrode to the drain electrode through a semi-conductor channel. The flow of current is controlled by the application of voltage on the gate electrode that creates an electric field, which in turn alters the conductivity between the source and drains control. BioFETs also work on the operational principles of FETs except that in bioFETs biorecognition layer replaces the gate electrode, which is capable of sensing target molecules. The biorecognition unit is an interface to the molecular channel which selectively reacts to the target molecules (ligands) by selectively binding them. It consists of receptor molecules that are tethered on the surface of the FET channel. The ligands are bound to the receptor molecules, which results in the accumulation or depletion of carriers in the semiconductor channel. In biorecognition layer field effect is created by intrinsic charges of the bound ligands and channel conductance is modulated by ligand binding Kuscu and Akan [5]. Fig. 2 shows an illustration of bioFETs based MC-Rx.

4.1. Communication parameters for BioFFET based MC-Rx

This work assumes a time-slotted molecular communication system with single transmitter and receiver pair that are perfectly synchronized in terms of time. The modulation scheme used for the communication system is M-ary concentration shift keying (M-CSK), such that the

Fig. 1. Internet of Bio nano things architecture where inbody bio chemical signals and sensory data is relayed through bio cyber interface through Internet to Medical server for further processing.

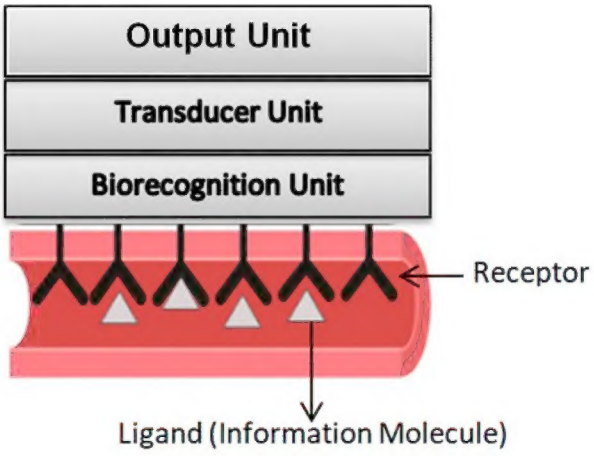


Fig. 2. Illustration of BioFET used as on skin biocyber interface, the ligands are extended into the blood vessel for capturing target molecules.

information is encoded into the molecular concentration. The transmission session initializes when the transmitter releases an N number of molecules as an input symbol for a single time slot. A straight microfluidic channel with a rectangular cross-section is considered as the propagation medium. The molecular transmitter is located at the entrance of the microfluidic channel, while Silicon NanoWire (SiNW) FET-based MC-Rx is located at the bottom of the channel at position $x = x_R$. The transducer channel of Mc-Rx is SiNW based and is covered by a thin oxide layer and surface receptors that are exposed to ligands of varying concentrations. The Mc-Rx employees ligand-receptor binding kinetics to sample the concentration of information molecules flowing over its surface. The flow mechanism of ligands is advection-diffusion and the MC-Rx is non-absorbent i.e., ligands bind to the receptors for a random amount of time and then unbind. As diffusion is considered as the propagation scheme, ISI (Inter Symbol Interference) might occur due to the long propagation time and spread over the x-axis. However, to prevent loss of generality in deriving the receiver model, this work assumes a memoryless propagation channel. The SiNW bioFET based Mc-Rx consists of three consecutive operational units. The biorecognition Unit (BU), Transduction Unit (TU), and Output Unit (OU). The biorecognition unit is an interface of Mc-Rx with the molecular channel and is responsible for selectively sensing some physical property of the target molecules, which in this case is molecular Kuscu and Akan [5]; Kuscu et al. [27] and generates a molecular recognition event (i.e., molecular reaction). The transduction unit then generates a processable electrical or biochemical signal based on the molecular reaction produced by BU. In bioFET based receiver, transduction is performed by intrinsic charges of bound ligands which modulates the gate potential of FET. Several ligand-receptor pairs can be used for BU of bioFETs, such as aptameter natural ligand, antibody-antigen, natural receptor/ligand Rogers [34]. Similarly, several types of semiconductors e.g., SINW, CNT, and graphene, have proven suitable as transduction units for bioFETs Poghossian and Schöning [35]. However, the basic operations of the biorecognition and transduction unit remain the same regardless of ligand-receptor pair and semiconductor types.

4.2. Molecular channel and communication system parameters

In this work, we consider the microfluidic channel MC channel. Here, the molecular encoded messages are transported *via* fluid flow-induced advection-diffusion, which may be created by a pressure difference between the two ends of the channel. Next, we will present the equations for the diffusion coefficient, equivalent capacitance, transconduction and, output current. These equations directly impact the output SNR and are considered important channel and communication system parameters. The detailed derivations of these equations are out of scope for this paper. Interested readers can find the derivations in Kuscu and Akan [5]. The output SNR of bioFET is given below:

$$SNR_{out,m} = \frac{\mu_{I_m}^2}{\sigma_{I_m}^2} \tag{1}$$

4.2.1. Diffusion coefficient

The transport dynamics of target molecules (ligands) inside the microfluidic channel are described through the advection-diffusion equation. The fluid flow is generated by the pressure difference between the two ends of the channel, flow is uni-directional along the x-axis and is assumed to be in steady-state i.e., there is no acceleration of the fluid Bicen and Akyildiz [36]. In this condition, fluid flow is considered as laminar and the total flow is formed by adding the contribution from each lamina Kuscu and Akan [5]. One dimensional advection-diffusion equation along the direction of the fluid flow can be written as

$$\frac{\partial \rho(x,t)}{\partial t} = D\frac{\partial^2 \rho(x,t)}{\partial x^2} - u\frac{\partial \rho(x,t)}{\partial x} \tag{2}$$

where $\rho(x, t)$ is the ligand concentration at position t and u is the maximum flow velocity. D is the effective diffusion coefficient taking into account the effect of Taylor-Aris type dispersion Bicen and Akyildiz [37]. For a channel with rectangular cross-section, it is given

$$D = \left(1 + \frac{(8.5u^2 h_{ch}^2 l_{ch}^2)}{210 D_0^2 (h_{ch}^2 + 2.4 l_{ch} h_{ch} + l_{ch}^2)}\right) D_0 \tag{3}$$

where the intrinsic diffusion coefficient is denoted by D_0 Bicen and Akyildiz [37]. Here, hch and lch denote the height and length of the microfluidic channel, respectively. The diffusion coefficient is an important characteristic that affects the SNR, the SNR decreases with an increase in the diffusion coefficient.

4.2.2. Equivalent capacitance

The equivalent capacitance of the transducer channel depends on three capacitances namely diffusion layer capacitance (C_{DL}), the capacitance of the oxide layer (C_{OX}), and the SiNW capacitance C_{NW}. Therefore, the equivalent capacitance of bioFET MC-Rx can be given by

$$C_{eq} = \left(\frac{1}{C_{OX}} + \frac{1}{C_{NW}}\right)^{-1} + C_{DL}. \tag{4}$$

where $C_{OX}=(\varepsilon_{ox}/t_{ox})w_R l_R.\varepsilon_{ox}$ is the relative permitivity and t_{ox} is thickness of oxide layer. $w_R = \pi r_R$ is the effective width of SiNW and l_R is the length of SiNW $C_{DL}=(\varepsilon_M/\lambda_D)w_R l_R$, where λ_D is the diffusion thickness covering the oxide layer. The effect of capacitance on SNR can be inferred as lower values of capacitance implies higher SNR. $C_{NW}= (\varepsilon_{Si}/\lambda_{nw})w_R l_R$ where ε_{Si} is the dielectric permittivity of the oxide layer and λ_{nw} is the thickness of double-layer created inside NW. The derivations of the above equations are out of the scope of this paper and can be found in Kuscu and Akan [5].

4.2.3. Transconductance of BioFET

The transconductance of bioFET can be obtained by taking derivative of source-drain current with respect to source-gate voltage Neamen [38]:

$$g_{FET} = \frac{\partial I_{SD}}{\partial V_{SG}} = \mu_p C_{OX}\frac{w_R}{l_R} V_{SD} \tag{5}$$

where V_{SG} is source to gate voltage,μ_p is carrier density, V_{SD} is source to drain voltage and $l_R = l_{ch}$. The higher values of g_{FET} imples more functional transconductance of the surface potential to the output current.

4.2.4. Output current of BioFET

The mean of output current is given by the following equation Kuscu and Akan [5]:

$$\mu I_m = g_{FET}\Psi_L N_R\left(1+\frac{K_D A_c h}{N_m}\sqrt{\frac{4\pi D x_R}{u}}\right)^{-1}. \quad (6)$$

where $\Psi_L = (q_{eff}xN_e^-)/C_{eq}$ is defined as surface potential of a single ligand Kuscu and Akan [5].

4.3. Attack vectors for bio cyber interface

A comprehensive literature survey in the field of security in bio cyber interface has revealed that research in this field is nascent. We were only able to find a few proposals Bakhshi and Shahid [39]; El-Fatyany et al. [13] regarding the security and privacy of bio cyber interface. Therefore, to investigate the possible attack types that are likely to affect the operation of bio cyber interface, we have investigated related fields like implanted medical devices (IMD) Camara, Peris-Lopez and Tapiador [40], Wireless sensor networks (WSN) Sharma, Bala and Verma [41] and Wireless Boday Area Networks (WBAN) Usman, Asghar, Ansari and Qaraqe [42]. Attacks to bio cyber interface can be life-threatening as the continuous monitoring applications depend on uninterrupted real-time data for medical prescriptions. The attacks in the bio cyber interface can be classified into three broad categories: 1)Reconnaissance – Illegal interception of information generated by bio cyber interface. 2) Exploits – these attacks take advantage of a known bug or design flaw in the system. 3)Denial-of-Service (DoS) – these attacks disrupt or deny access to a service or resource.

Other possible attacks on bioFETs are briefly described below:

4.3.1. Sentry and blackhole attacks

Bio FETs work on the principles of ligand binding through the charging of electrodes. The attacker can launch a sentry attack to repel required ligands or a black hole attack to attract unwanted ligands to bind to the receptor to affect the current control. The changes in external current control can cause the Bio FET-based bio cyber interface to exhibit unwanted behavior. The feature "output current" is specifically more weighted in case of sentry and blackhole attacks. Moreover, to counter these types of attacks, the dataset can be sanitized by rejecting the features with abnormal values and only keeping the values that lie in the normal range.

4.3.2. Eavesdropping

Eavesdropping refers to silently intercepting the communication between two entities. This attack can invade the privacy of patients as the information communicated by the bio cyber interface is of sensitive and confidential nature. The information contains location, device ID, and physiological body parameters. The eavesdropped information can be used to launch further attacks. An abnormal value of output current feature will notify that the communication channel is being intercepted by an adversary.

4.3.3. Man-In-The-Middle attack

A man-In-The-Middle attack can be launched when an adversary illegally enters the communication channel and impersonate it to be the legitimate bio cyber interface. After getting illegal access to the channel, an attacker can manipulate the recorded data received from the bio cyber interface and send altered records to the healthcare provider, which can result in inappropriate medical prescriptions. Abnormal values of transconductance and diffusion coefficient will aid in detecting this type of attack.

4.3.4. Device tampering

This attack refers to causing physical harm to the device or replacing it with a maliciously coded device to send fake data to the healthcare provider. This attack is possible only when the attacker is in close vicinity of the device. All the features used in this work can be used to detect this attack.

4.3.5. Firmware attack

Bio cyber interface devices will need periodic firmware updates like any other IoT device to function properly. The attacker can send fake firmware update messages to alter the software configuration of the bio cyber interface. Latest firmware and future updations must be embedded in the device and strong authentication control services must be applied to circumvent this attack.

5. The proposed system model

The proposed security framework differentiates between the normal and anomalous behavior of bioFET based MC-Rx, through features that represent a statistical behavior of the network. The data is processed to extract the features for bioFET based MC-Rx. The corresponding features are expected to represent class labels as normal or anomalous. The proposed security framework consists of four modules namely (i) Data pre-processor, (ii) Feature Profiler (iii) PSO-based ANN Classifier and (iv)Anomaly Detector. A high-level schematic representation of the proposed security framework is presented in Fig. 3 and a detailed flow chart of the proposed model is presented in Fig. 4.

5.1. Data pre-processor

The data pre-processor module is responsible for data collection and sanitization. In this study, the data was generated synthetically, through information-theoretic system parameters of bioFET based MC-Rx. The proposed scheme mainly utilizes the channel and communication criterion of bioFET based MC-Rx. The criterion includes diffusion coefficient, equivalent capacitance, transconductance, and output current, details of which are discussed in Section 4.2. The data was generated by computer-based simulations for the BioFET communication features in equations ((3) to (6)). The equations were taken directly

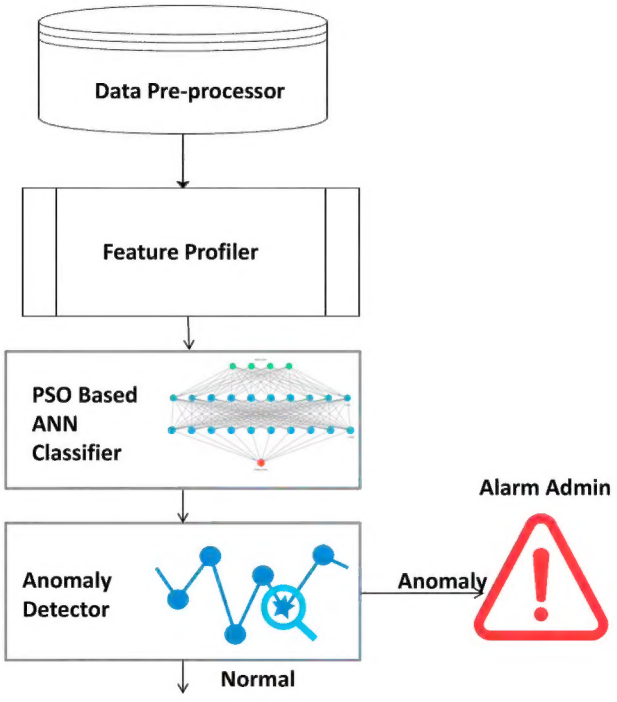


Fig. 3. A schematic representation of the proposed PSO based ANN security frame work.

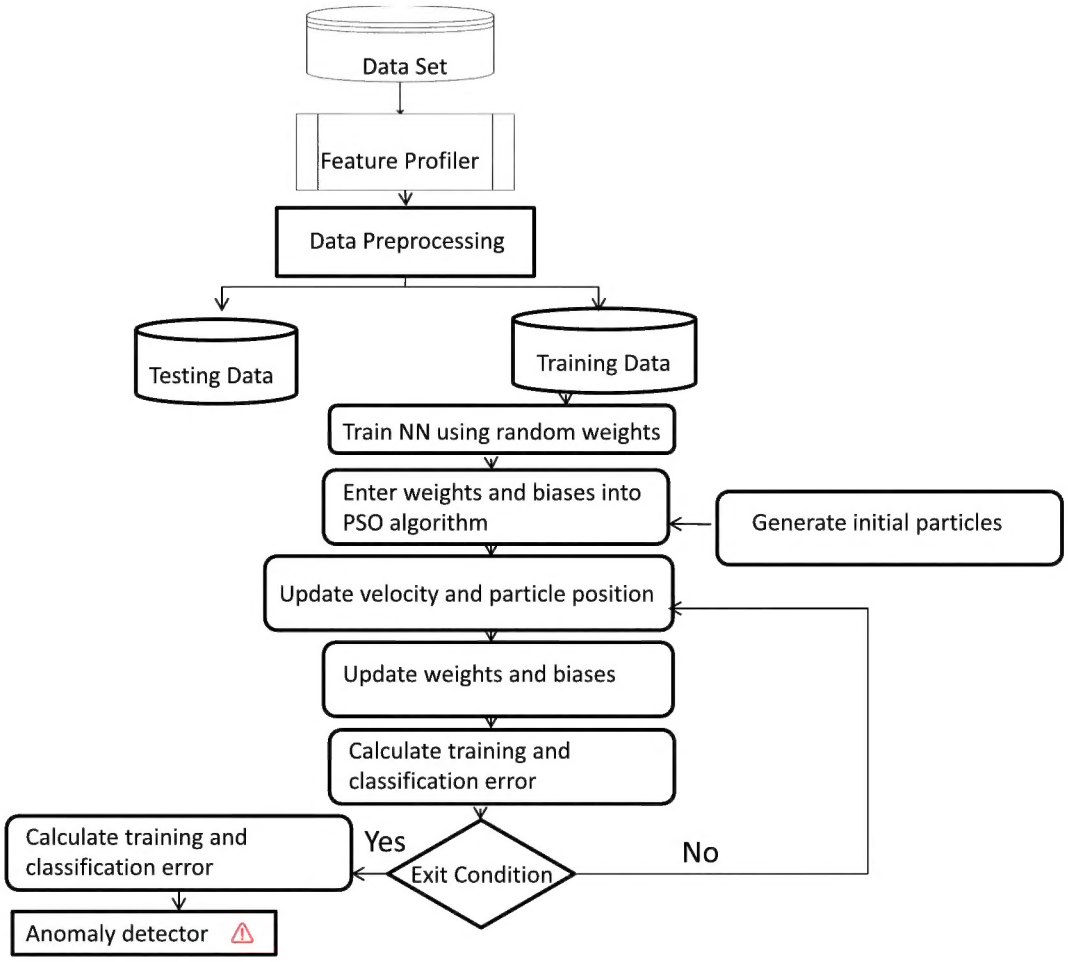


Fig. 4. Flow chart of proposed model.

from Kuscu and Akan [5], which provides information-theoretic modeling for bioFET based MC-Rx. The parameters for simulations of equation ((3) to (6)) are presented in Table 1. One million records were generated using the randomization function for each criterion. Approximately 50% of the values were generated for the normal operation of bioFET based MC-Rx. The other 50% were given a standard deviation of up to 5% to represent anticipated anomalies. The data was split into a 70:30 train: test ratio.

In this phase, a feature vector P is defined which contains the characteristics of communication channel C between biocyber interface and Internet I. An abstract equation for the same is given below Bakhshi and Shahid [39]:

$$P_{C \to I} = \{F_i\} \tag{7}$$

Table 1
Simulation parameters for equations (3)–(6).

Parameter	Description	Value
u	Average flow velocity	$10 - 50$ μm/s
D_0	Diffusion co-efficient of ligands	$1 \times 10^{-10} - 2 \times 10^{-10}\ m^2/s$
h_{ch}	Microfluidic channel height	0.1–20 μm
l_{ch}	Microfluidic channel width	$5 - 20$ μm
V_{SD}	Source Drain Voltage	0.1–0.3 V
V_{SG}	Source Gate Voltage	0.4–0.6 V
μ_p	Effective mobility of carriers	$160 - 500$ cm^2/V
N_e^-	Average number of electrons in a ligand	3–4
$\varepsilon_{ox}/\varepsilon_0$	Relative permittivity of SiO2 layer	3.9–4.3
t_{ox}	Thickness of oxide layer	$1.5 - 3$ nm
r_R	SiNW radius	$10 - 15$ nm

Where F is features and i represents the number of attributes associated with the communication channel C. The feature vector P is then forwarded to the feature profiler module.

5.2. Feature profiler

The future profiler accepts feature vector P as an input. As MC and IoBNT are novel communication paradigms, therefore its datasets from a security perspective are nascent on important machine learning dataset sources. However, some works in the literature have utilized computer-simulated data for the authentication of MC. In our previous work, we used Channel Impulse Response (CIR) as a feature for authentication in diffusion-based MC Zafar et al. [24]. Another work utilized distance as a feature to generate cipher keys for eavesdropping prevention in MC. Similar work to our proposed work describes three bio cyber interfacing technologies based on (i)Bioluminescence, (ii)Redox modality, and BioFET based bio cyber interfacing. The features for ML-based parameter profiling is done according to distinct operational features of each technology such as thermal reading and photo luminosity are used as features for Bioluminescence based technology, voltage feature is used for Redox modality and, current and voltage are used as features for BioFET technology to identify outliers and anomalous operation. In traditional ML-based applications, automated feature selection algorithms are used e.g., supervised feature selection methods like filter models, wrapper models, and embedded models Tang, Alelyani and Liu [43]. Feature selection for this novel communication paradigm of IoBNT and MC was the most complex task of the proposed work due to the unavailability of datasets. Feature selection in the proposed model is

done according to their relevance to the communication mechanism of BioFET based MC antennas. This work is based on the BioFET based MC receiver model proposed in Kuscu and Akan [5]. Therefore, the features selected for classification in our model strictly depend on the molecular, receiver, and communication system parameters of BioFET based receiver defined in Kuscu and Akan [5]. The main function of BioFET based MC receiver is to convert received molecular signals into electrical current, which in turn drives the electromagnetic signal for cyber interfacing. We have selected the distinct operational features of BioFET based bio cyber interface, an abnormality to the same can affect the normal functioning and output of the device. Moreover, these features also affect the SNR Kuscu and Akan [5] and capacityKuscu and Akan [44] of BioFET based MC receiver. Features selected for the proposed work include diffusion coefficient, equivalence capacitance, transconductance, and output current. **Diffusion Co-efficient**: The diffusion coefficient is an important molecular parameter that affects the SNR and overall performance of BioFET based MC receiver. The diffusion coefficient is related to the content of the molecular message. Abnormality in the parameters of diffusion co-efficient can tamper the original message encoded as the molecular signal. This will affect an important security goal "integrity" from the CIA (Confidentiality Integrity Availability) security triad. **Equivalence Capacitance**: Equivalence Capacitance is another important feature to determine the performance of BioFET, as the change in the small-signal capacitance due to a shift in the threshold voltage can affect the operation of BioFET.Moreover, the unwanted reactance of the equivalence capacitance resulted due to anomalous parameter values, can significantly affect the bioFET hence causing to depict behavior like Denial of Service (DoS), hence causing unavailability. **Transconductance**: Transconductance is another expression of BioFET performance, the larger the transconductance figure for a device, the greater the gain it is capable of delivering. Transconductance (g_{FET}) is a sensing metric in bioFET which provides sensitive molecular detection. Interference in the input voltage of g_{FET} affects the values of current at the output terminal, hence producing abnormal values. **Output current**: Output current is the most important feature which is used to drive the bioFET device to produce an electromagnetic signal for bio cyber interfacing. Current has already been proved as a feature for securing BioFET based biocyber interface by authors in Bakhshi and Shahid [39]. Normal range and values of these features are calculated using equations ((3) to (6)) using simulation parameters in Table 1. Abnormal values of these features will imply an anomalous operation of BioFET, which means the bioFET is manipulated by an intruder.

5.3. PSO based ANN classifier

Artificial Neural network classification has been proved effective in the field of network security, especially in the problems of network intrusion detection Almiani, AbuGhazleh, Al-Rahayfeh and Razaque [45]; Almiani, AbuGhazleh, Al-Rahayfeh, Atiewi and Razaque [46]; Kang and Kang [47]. ANNs are self-adaptive and can capture complex relationships between dependant and independent variables without prior knowledge. ANNs can overcome the complexities of model building associated with traditional classification techniques like decision trees and k nearest neighbors. Moreover, ANNs have an additional ability to adapt to the underlying system model as compared to conventional classification methods like logistic regression and discriminant analysisShenfield, Day and Ayesh [48]. These properties of ANNs make them an ideal candidate to be used in network security frameworks. Traditional ANNs suffer from drawbacks such as trapped in local minima and overfitting. To overcome the problem of local minima, we have implemented PSO based ANN classifier that yields to global minima. For the ultimate goal of detecting the anticipated anomalies, accounting for malicious operations, a Multi-Perceptron Neural Network is utilized. The dataset contains approximately one million data instances, with four features having binary targets. The dataset was randomly split into two sets; training dataset and testing dataset. From the randomly organized data, 700000 instances were dedicated for training which is 70% of the total data records, whereas the remaining 30% which equals 300000 data records was devoted to testing the trained model. The data set was normalized using standard scalar to improve its effectiveness. The proposed network inputs 4-dimensional input vectors and outputs a one-dimensional vector which represents the decision for normal or anomalous data. Two hidden layers were used, containing 100 neural nodes each. Fig. 5 presents the specifications of ANN described above. For optimization of the proposed ANN, Particle Swarm Optimizer (PSO) was implemented.

Particle Swarm Optimization (PSO) is a bio-inspired global heuristic optimization algorithm Bai [49]. PSO is based on the swarm intelligence and search optimization process of bird flocks. As birds flock search for food, they keep storing and communicating the best place for food. Similarly, in PSO the particles search for the most optimal solution in a *D*-dimensional search space and keep searching for the best and optimistic solution until they find the global best. The initial population of the particles is randomly distributed over the search space. The particles move continuously in the search space to find the optimal solution. The particle's motion depends on three factors,(i) current position of the particle, (ii) personal best (P_{best}) position the particle has been on so far and (iii)Global best (G_{best}) position of entire series of all particles Engelbrecht [50]. New position of each particle can be calculated as follows Saljoughi, Mehrvarz and Mirvaziri [51]:

$$curr_{pos}(t+1) = curr_{pos}(t) + v(t+1) \tag{8}$$

where $curr_{pos}\ (t+1)$ calculates the next position, and $curr_{pos}$ represents the present position of the particle. $v\ (t+1)$ is velocity function which specifies the direction of particle motion and can be defined as follows:

$$\begin{aligned} v(t+1) = w * v(t) + C_1 * r(0,1) * [P_{best}(t)] \\ [-curr_{pos}(t)] + C_2 * r(0,1) * [G_{best}(t) - curr_{pos}(t)] \end{aligned} \tag{9}$$

where t is the tth iteration in the evolution process, w is the inertia weight that represents the impact of previous velocities on the current velocity, C_1 and C_2 are learning constants such that C_1 implies personal weight and C_2 implies global weight. The r variable represents random distribution of numbers greater than or equal to 0 and less than 1. PSO algorithm is given below:

Algorithm 1. Particle Swarm Optimization Algorithm.

Algorithm 1 Particle Swarm Optimization Algorithm

Initialization
$P_{best}, v, curr_{pos} \leftarrow \emptyset$
Set each particle to random state
$N \leftarrow iterate_{max}$
for $i \leftarrow 0$ to N **do**
  for $i \leftarrow 0$ to $iter_{max}$ **do**
    Compute fitness value
    if $f(curr_{pos}[particle]) < f(P_{best}[particle])$ **then**
      $SetP_{best}[particle] = curr_{pos}[particle]$
    end if
    if $f(P_{best}[particle]) < f(G_{best})$ **then**
      $SetG_{best} = P_{best}[particle]$
    end if
  end for
  Update velocity according eq (8)
  Update current position according to eq (9)
end for
return G_{best}

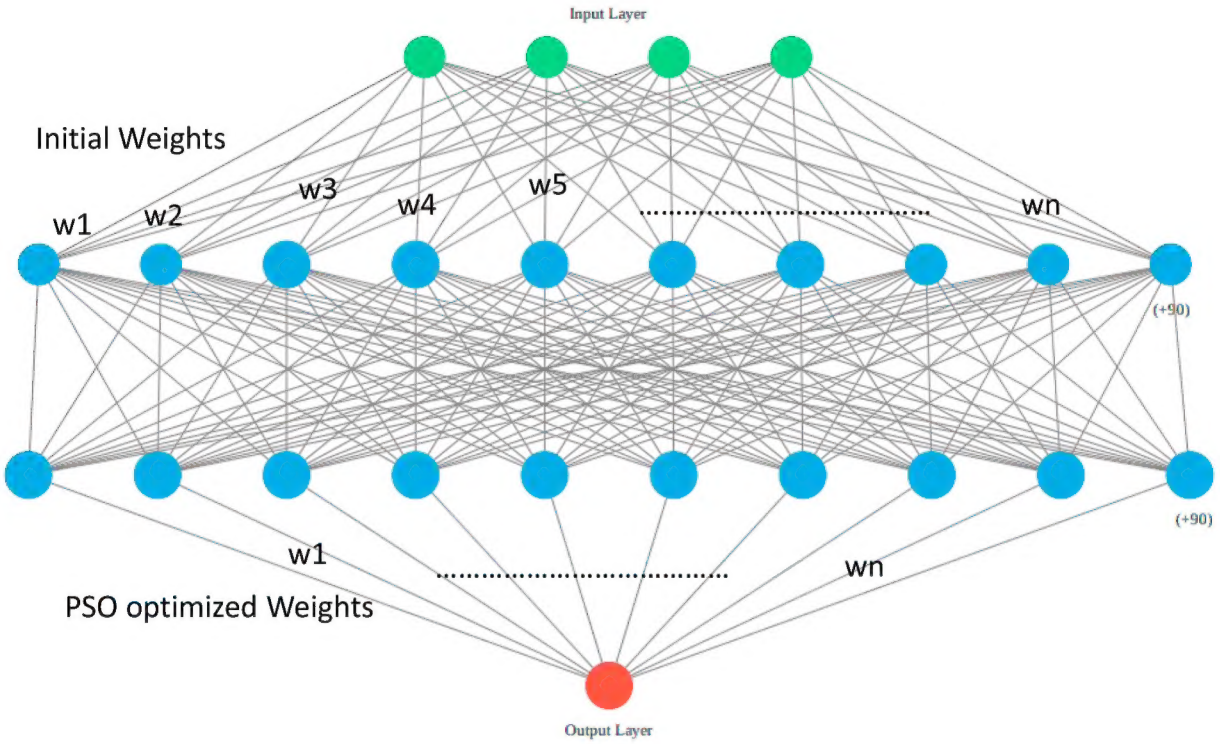


Fig. 5. Visualization of the topology of adopted Neural Network.

5.3.1. Parameter tuning for PSO: a practical example

The selection of parameter values for PSO directly impacts the rate of convergence. In this work, trial and error experimentation is performed to find the optimal PSO parameters that yield the fastest neural network convergence. The optimal parameters can be determined by varying the values of variables and constants in equations (8) and (9), to increase the efficiency of anomaly detection in Bio-FET cyber interfaces. Inertia weight is an important parameter signifying the balance between local and global searches and affecting algorithm convergence. Since anomaly detection is a real-time phenomenon, the least number of iterations to yield the optimal solution is required. Therefore, based on prior research Gudise and Venayagamoorthy [52], the inertia weight (w) used is between a minimum and maximum of 0.2 and 1.2. Similarly, velocity reflects particle distance traveled at each iteration, depending on previous best found for the particle and the entire swarm memory and is set to maximum value of 4. The search space is varied between (−2, 2) and (−200, 200). Swam size which is typically restricted to a value between 20 and 50 particles in previous literature for the majority of PSO applications and variants. Anomaly detection based on limited features can be considered as relatively unimodal suggesting swarm space selection be set closer to the minimum value of this classical 20–50 range. In present experimentation it was therefore, set towards the lower end at the start, however, varied up to 1000 to account for the fact that practical anomaly detection might report higher efficiency at larger swarm size values in rough (er) search spaces. Constants, representing trust parameters of self-confidence and neighbour confidence (C_1, C_2) ranged between 0 and 3. The parameter values were varied along the course of experimentation to seek parameter optimality. The optimal parameters for PSO based optimization can be found in Section 6.4.

5.3.2. Training steps for PSO based ANN classifier

First of all the input data set is divided into two categories: training dataset and testing dataset. The training process starts on training dataset with random weights which are then optimized using the PSO algorithm. The training process is repeated until G-best is obtained. The steps included in PSO based ANN classifier are as follows:

1. Train neural network through an initial set of random weights and biases. The weighted sum of inputs is computed as follows:

$$Y = \sum(weight * input) + bias \tag{10}$$

2. Initialize PSO variables with the set of weights and biases which are obtained from training in the first step.
3. Calculate the error of classification and update the weights and biases with optimized values in each repetition of the algorithm. In each repetition, particles move towards G_{best} position.
4. Replace velocity and position with optimal ones.
5. Replace the weights and biases in each stage with optimal weights.
6. Once G_{best} is achieved upon meeting the exit condition (a good fitness value or a maximum number of iterations), NN is trained with optimal weights and tested with test data. If an anomaly is detected it is passed to the anomaly detector.

The graphical topology of adopted ANN for this work is presented in Fig. 5.

5.4. Anomaly detector phase

The anomaly detector works in real-time to compute the trained parameters and make a binary decision. In case of detecting malicious activity, the anomaly sends an alarm signal to the admin.

6. Simulations and results

6.1. Data generation

This section describes the synthetic data generation for the dataset, and detailed parameter-based profiling results for bioFET based bio cyber. Firstly, computer-based simulations were performed to generate synthetic data for communication features in equations ((3) to (6)). The simulation parameters for solving equations ((3) to (6)) were obtained from the literature review and are given in Table 1. This procedure uses

the values lying within the defined range of simulation parameters. For example, to generate normal values of the feature "Diffusion co-efficient", the values of variables D_0, l_{ch}, h_{ch} and u are taken from the pre-defined range of each variable presented in Table 1. The usage of synthetic data can be justified by the unavailability of real-time data for MC and bioFET based bio cyber interface. The datasets were searched on popular database sources like IEEEdataport, kaggle,5. UCI Machine Learning Repository and github. But due to the novelty of IoBNT and BioFET based MC receivers, there were no datasets available.

6.1.1. Attack data generation

To generate the attack data, the values of each parameter of the features (Diffusion co-efficient, Equivalence Capacitance, Trans-conductance and Output Current) were taken from out of pre-defined value range. For example, for attack data of diffusion coefficient, value D_0 did not lie between the normal range ($1 \times 10^{-10} - 2 \times 10^{-10}$ m^2/s). Similarly, the values of parameters for each feature were taken outside the normally defined range. Moreover, for further caution in distinguishing between normal and abnormal values, we adopted the approach used by a similar work Bakhshi and Shahid [39]. In this work standard deviation of 5% was added to the primary features to represent anticipated anomalies. This will distinguish the normal class data from abnormal data. Currently, we are using a 5% deviation technique to generate attack data but in the future and upon implementation of practicable IoBNT, attack data will be recorded based on real-time traffic.

Next, the generated data was subjected to ANN for binary classification.

6.2. Simulation setup

We began by collecting approximately one million data samples from the data generation phase. We approximate the number of data samples because we ran our experimentation multiple times, added additional data samples, and divided the data into random training and testing data sets. One set is for training the neural network and the second set is for testing the accuracy of the trained network. Python programming language is used for neural network simulation setup in this work. Specifically, Google Colaboratory (colab) was utilized which is a product from Google research. The specifications of GPU from colab are as follows: GPU memory: 12GB/16 GB, GPU Memory Clock 0.82GHz/1.59 GHz and RAM 12 GB. Colab was utilized due to its free access to computing resources especially GPU.

6.3. Results

The performance of the proposed security framework is evaluated through the popular performance pentagon i.e., Accuracy, Precision, Recall, F-Measure, and False alarm rate which are predominantly utilized for network security performance evaluation in literatureAlmiani et al. [45].

Pentagon metrics can be defined mathematically as in equations (11)–(15).

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FN + FP)} \tag{11}$$

where accuracy defines the ratio of number of correct predictions to the total number of input samples.

$$Precision = \frac{TP}{(TP + FP)} \tag{12}$$

where Precision represents the fraction of correctly classified records to that totally classified as malicious.

$$Recall(Sensitivity) = \frac{TP}{(TP + FN)} \tag{13}$$

where Recall represents the fraction of normal data records that are correctly classified as normal, with respect to all normal data records records.

$$FPR(FalsePositiveRate) = \frac{FP}{(FP + TN)} \tag{14}$$

where FPR represents the proportion of malicious data records that are mistakenly classified as normal, concerning all malicious data records. The false positive rate measures the fake alarms response of the system.

$$Fmeasure = \frac{2}{\frac{1}{Recall} + \frac{1}{Precision}} \tag{15}$$

F measure is the Harmonic Mean between precision and recall. The range for the F1 measure is [0, 1]. *True Negatives* (TN) represents the number of normal data records that are classified correctly as normal. *True Positives* (TP) represents the number of anomalous data records that are classified correctly as anomalous. Whereas *False Positive* represents the number of anomalous data records that have been misclassified as normal and *False Positive* corresponds to the number of normal data records that have been misclassified as anomalous. Fig. 6 shows the accuracy graph of the proposed model.

The accuracy of the proposed framework yields to 98.9%, Precision equals 99%, Recall score is 98.03%, F measure is 99% and FPR is 99%. The ROC (Receiver Operating Curve) plots two parameters; TPR (Recall) and FPR(False Positive Rate). ROC is also plotted to evaluate the performance of our proposed model. AUC (Area Under the curve) of our model equals a higher classification value of 0.99. The ROC graph of our proposed model is presented in Fig. 7.

6.4. Comparison between results of adam-based optimization and PSO-based optimization

The results of the PSO-based ANN classifier were compared with an ANN model that uses Adam gradient descent as an activation function. For PSO based optimization the optimal value for inertia was determined to be 0.7 with a velocity of 2, and a search space value of (−150, 150) giving best results. The swarm size of 100 yielded higher performance as compared to lower values. Constants $C_1 = 1.4$ and $C_2 = 1.4$ reported best results with self-confidence and neighbour confidence existing in a good balance ($C_1 = C_2$), suggesting an equal mix of smooth and rough in the search space. Lets solve equations (8) and (9) to see the results after PSO weight optimization. We suppose particle's current position is (3.0,4.0), $P_{best} = (2.5, 3.6)$ and $G_{best} = (2.3, 3.4)$. Now putting the values in equations (8) and (9) to find the PSO optimized weights:

$$\begin{aligned} v(t+1) &= (0.7^{*}2) + (1.4^{*}0.5^{*}\{2.5, 3.6\} - \{3.0, 4.0\}) + \\ &\quad (1.4^{*}0.6^{*}\{2.3, 3.4\} - \{3.0, 4.0\}) \\ &= \{-0.70, -1.05\} + \{-0.35, -0.28\} + \{-0.59, -0.50\} \\ &= \{-1.64, -1.83\}. \end{aligned}$$

$$curr_{pos}(t+1) = \{3.0, 4.0\} + \{-1.64, -1.83\} = \{1.36, 2.17\}.$$

It can be observed that the current position of the particle is improved from (3.0,4.0) to (1.36,2.17) after executing the update process. Moreover, the best position vector found by the PSO will be the weight and bias parameters of the network and use the trained weights to perform class predictions. An Adam gradient descent optimizer was replaced by PSO for result comparison. Rectified linear unit (ReLU) was used after each hidden layer to provide non-linearity. Since the proposed work is manipulated as a binary classification problem, therefore, the sigmoid function is used for the output layer. ReLU is defined in equation (16) and sigmoid function is defined in equation (17) below Baldi and Vershynin [14]:

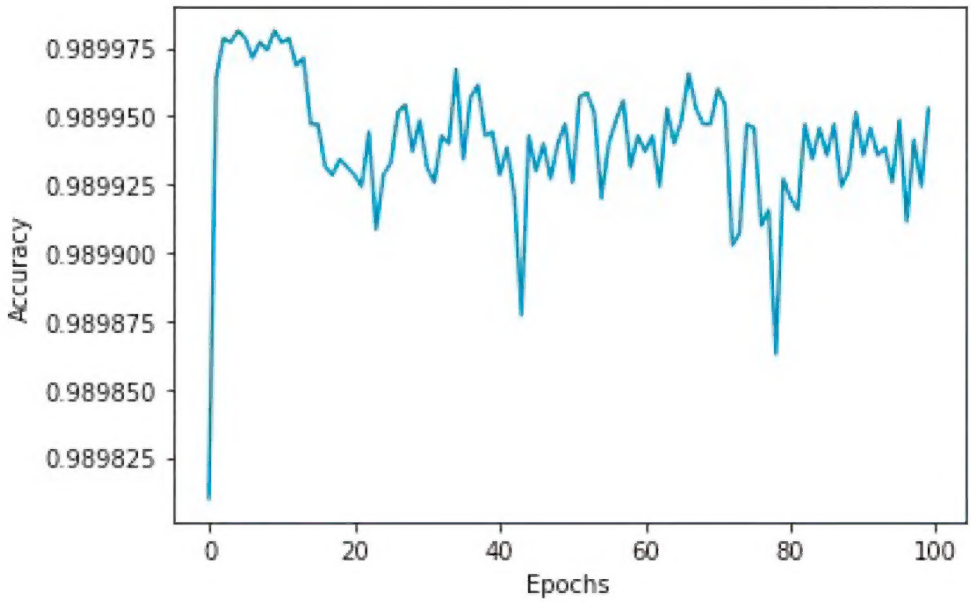


Fig. 6. Accuracy graph of the proposed model.

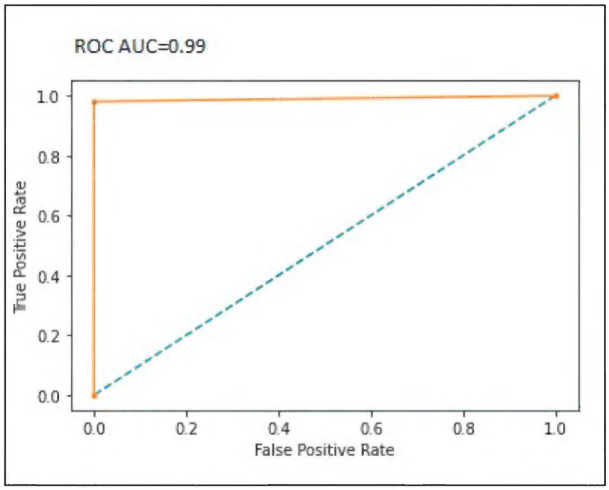


Fig. 7. ROC graph of the proposed model.

$$R(x') = \max(0, x') \tag{16}$$

$$f(x') = \frac{1}{1 + e^{-x'}} \tag{17}$$

Fig. 8 shows the comparison of accuracy between PSO-based ANN and Adam-based ANN.

The results reveal that our proposed PSO-based ANN classifier outperforms Adam-based ANN with an accuracy of 98.9% and precision of 99%.Other performance metrics of both the models are presented in Table 2.

7. Conclusion

Internet of Bio-Nano Things is an emerging ICT domain that offers the most promising applications in advanced healthcare and the biomedical domain. The most promising biomedical applications of IoBNT include early detection of serious diseases like cancer and remote diagnosis and treatments of patients via targeted drug delivery. A successful realization of this novel paradigm depends on the

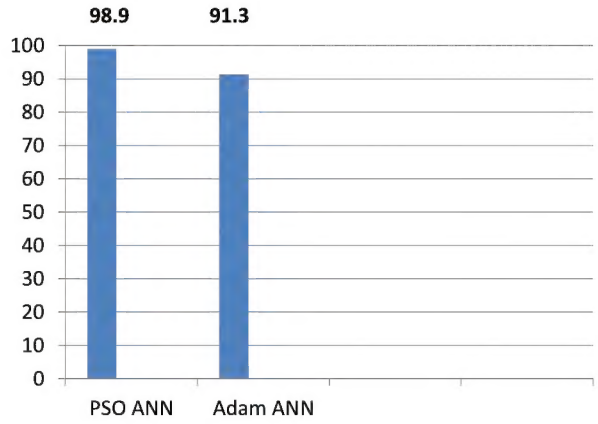


Fig. 8. Comparison of accuracy between PSO based ANN and Adam based ANN.

Table 2
Comparison between performance metrics for proposed security framework and Adam based ANN classifier.

Parameter	Adam based ANN Value (%)	PSO based ANN Value (%)
Accuracy	91.3	98.9
Precision	92.7	99
Recall Score	90.6	98.03
F-Measure	91.8	99
False Alarm rate	94.13	99

implementation of a bio cyber interface that bridges the technological gap between the intra-body biological environment and the electrical cyber world. The design and integration of device components depend on individual IoBNT applications, for example for sensing applications relevant sensors must be integrated for sensing individual biochemical substances like pH, sodium, calcium, etc. Similarly, for drug delivery applications drug reservoirs must be integrated within the device.

Yet, this ability can pose major security threats to the safety and security of patients. There is always a chance that these devices will be accessed by adversaries with malicious intent. Therefore, mechanisms to

provide security to these devices must be investigated at an early stage of the application development. In this paper, we proposed a framework for the security of the bio cyber interface of IoBNT. We have implemented a PSO-based optimization function to be utilized by Artificial Neural Networks, which can provide optimized classification between legitimate and malicious devices. ANNs can adapt to the underlying system model as compared to conventional classification methods like logistic regression and discriminant analysisShenfield et al. [48]. These properties of ANNs make them an ideal candidate to be used in network security frameworks. Traditional ANNs suffer from drawbacks such as trapped in local minima and overfitting. To overcome the problem of local minima, we have implemented PSO based ANN classifier that yields to global minima. The utilized PSO-based ANN classifier provides increased accuracy and decreased classification error. The results have shown a better accuracy of 98.9% when compared to the Adam optimization function.

Declaration of competing interest

The authors declare no conflict of interest in the submission titled "Securing Bio-Cyber Interface for the Internet of Bio-Nano Things using Particle Swarm Optimization and Artificial Neural Networks based Parameter Profiling".

References

[1] I.F. Akyildiz, M. Pierobon, S. Balasubramaniam, Y. Koucheryavy, The internet of bio-nano things, IEEE Commun. Mag. 53 (2015) 32–40.

[2] E. Kim, J. Li, M. Kang, D.L. Kelly, S. Chen, A. Napolitano, L. Panzella, X. Shi, K. Yan, S. Wu, et al., Redox is a global biodevice information processing modality, Proc. IEEE 107 (2019) 1402–1424.

[3] S.M. Abd El-atty, R. Bidar, E.S.M. El-Rabaie, Molcom system with downlink/uplink biocyber interface for internet of bio-nanothings, Int. J. Commun. Syst. 33 (2020), e4171.

[4] L. Grebenstein, J. Kirchner, R.S. Peixoto, W. Zimmermann, F. Irnstorfer, W. Wicke, A. Ahmadzadeh, V. Jamali, G. Fischer, R. Weigel, et al., Biological optical-to-chemical signal conversion interface: a small-scale modulator for molecular communications, IEEE Trans. NanoBioscience 18 (2018) 31–42.

[5] M. Kuscu, O.B. Akan, Modeling and analysis of sinw fet-based molecular communication receiver, IEEE Trans. Commun. 64 (2016) 3708–3721.

[6] D. Sadighbayan, M. Hasanzadeh, E. Ghafar-Zadeh, Biosensing based on field-effect transistors (fet): recent progress and challenges, Trac. Trends Anal. Chem. (2020) 116067.

[7] S. Park, J. Choi, M. Jeun, Y. Kim, S.S. Yuk, S.K. Kim, C.S. Song, S. Lee, K.H. Lee, Detection of avian influenza virus from cloacal swabs using a disposable well gate fet sensor, Adv. Healthc. Mater. 6 (2017) 1700371.

[8] Y. Chen, R. Ren, H. Pu, X. Guo, J. Chang, G. Zhou, S. Mao, M. Kron, J. Chen, Field-effect transistor biosensor for rapid detection of ebola antigen, Sci. Rep. 7 (2017) 1–8.

[9] M. Salehirozveh, P. Dehghani, M. Zimmermann, V.A. Roy, H. Heidari, Graphene field effect transistor biosensors based on aptamer for amyloid-β detection, IEEE Sensor. J. 20 (2020) 12488–12494.

[10] V.A. Pham Ba, Y.M. Han, Y. Cho, T. Kim, B.Y. Lee, J.S. Kim, S. Hong, Modified floating electrode-based sensors for the quantitative monitoring of drug effects on cytokine levels related with inflammatory bowel diseases, ACS Appl. Mater. Interfaces 10 (2018) 17100–17106.

[11] V.A. Pham Ba, D.g. Cho, S. Hong, Nafion-radical hybrid films on carbon nanotube transistors for monitoring antipsychotic drug effects on stimulated dopamine release, ACS Appl. Mater. Interfaces 11 (2019) 9716–9723.

[12] S. Zafar, M. Nazir, T. Bakhshi, H.A. Khattak, S. Khan, M. Bilal, K.K.R. Choo, K. S. Kwak, A. Sabah, A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things, IEEE Access 9 (2021) 93529–93566, https://doi.org/10.1109/ACCESS.2021.3093442.

[13] A. El-Fatyany, H. Wang, S.M. Abd El-atty, M. Khan, Biocyber interface-based privacy for internet of bio-nano things, Wireless Pers. Commun. 114 (2020) 1465–1483.

[14] P. Baldi, R. Vershynin, The capacity of feedforward neural networks, Neural Network. 116 (2019) 288–311.

[15] V. Loscri, C. Marchal, N. Mitton, G. Fortino, A.V. Vasilakos, Security and privacy in molecular communication and networking: opportunities and challenges, IEEE Trans. NanoBioscience 13 (2014) 198–207.

[16] A. Giaretta, S. Balasubramaniam, M. Conti, Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks, IEEE Trans. Inf. Forensics Secur. 11 (2015) 665–676.

[17] W. Guo, Z. Wei, B. Li, Secure internet-of-nano things for targeted drug delivery: distance-based molecular cipher keys, in: 2020 IEEE 5th Middle East and Africa Conference on Biomedical Engineering (MECBME), IEEE, 2020, pp. 1–6.

[18] F. Dressler, F. Kargl, Towards security in nano-communication: challenges and opportunities, Nano Commun. Netw. 3 (2012) 151–160.

[19] F. Dressler, F. Kargl, Security in nano communication: challenges and open research issues, in: 2012 IEEE International Conference on Communications (ICC), IEEE, 2012, pp. 6183–6187.

[20] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, M. Pierobon, Secrecy capacity and secure distance for diffusion-based molecular communication systems, IEEE Access 7 (2019) 110687–110697.

[21] S.P. Singh, S. Yadav, S. Mishra, Secrecy capacity of diffusive molecular communication under biological spherical environment, in: Proceedings of the 1st ACM International Workshop on Nanoscale Computing, Communication, and Applications, 2020, pp. 33–38.

[22] G. Sharma, N. Pandey, A. Singh, R.K. Mallik, Secrecy optimization for diffusion-based molecular timing channels, IEEE Trans. Mol., Biol. Multi-Scale Commun. (2021), https://doi.org/10.1109/TMBMC.2021.3054907.

[23] W. Guo, Y. Deng, B. Li, C. Zhao, A. Nallanathan, Eavesdropper localization in random walk channels, IEEE Commun. Lett. 20 (2016) 1776–1779.

[24] S. Zafar, W. Aman, M.M.U. Rahman, A. Alomainy, Q.H. Abbasi, Channel impulse response-based physical layer authentication in a diffusion-based molecular communication system, in: 2019 UK/China Emerging Technologies (UCET), IEEE, 2019, pp. 1–2.

[25] T. Nakano, M.J. Moore, F. Wei, A.V. Vasilakos, J. Shuai, Molecular communication and networking: opportunities and challenges, IEEE Trans. NanoBioscience 11 (2012) 135–148, https://doi.org/10.1109/TNB.2012.2191570.

[26] B. Atakan, O.B. Akan, S. Balasubramaniam, Body area nanonetworks with molecular communications in nanomedicine, IEEE Commun. Mag. 50 (2012) 28–34.

[27] M. Kuscu, E. Dinc, B.A. Bilgin, H. Ramezani, O.B. Akan, Transmitter and receiver architectures for molecular communications: a survey on physical design with modulation, coding, and detection techniques, Proc. IEEE 107 (2019) 1302–1341.

[28] M. Kuscu, O.B. Akan, On the physical design of molecular communication receiver based on nanoscale biosensors, IEEE Sensor. J. 16 (2016) 2228–2243.

[29] J. Shan, J. Li, X. Chu, M. Xu, F. Jin, X. Wang, L. Ma, X. Fang, Z. Wei, X. Wang, High sensitivity glucose detection at extremely low concentrations using a mos 2-based field-effect transistor, RSC Adv. 8 (2018) 7942–7948.

[30] S. Xu, J. Zhan, B. Man, S. Jiang, W. Yue, S. Gao, C. Guo, H. Liu, Z. Li, J. Wang, et al., Real-time reliable determination of binding kinetics of dna hybridization using a multi-channel graphene biosensor, Nat. Commun. 8 (2017) 14902.

[31] B. Kim, H.S. Song, H.J. Jin, E.J. Park, S.H. Lee, B.Y. Lee, T.H. Park, S. Hong, Highly selective and sensitive detection of neurotransmitters using receptor-modified single-walled carbon nanotube sensors, Nanotechnology 24 (2013) 285501.

[32] N. Garralda, I. Llatser, A. Cabellos-Aparicio, E. Alarcón, M. Pierobon, Diffusion-based physical channel identification in molecular nanonetworks, Nano Commun. Netw. 2 (2011) 196–204.

[33] N. Farsad, A.W. Eckford, S. Hiyama, Design and optimizing of on-chip kinesin substrates for molecular communication, IEEE Trans. Nanotechnol. 14 (2015) 699–708.

[34] K.R. Rogers, Principles of affinity-based biosensors, Mol. Biotechnol. 14 (2000) 109–129.

[35] A. Poghossian, M.J. Schöning, Label-free sensing of biomolecules with field-effect devices for clinical applications, Electroanalysis 26 (2014) 1197–1213.

[36] A.O. Bicen, I.F. Akyildiz, System-theoretic analysis and least-squares design of microfluidic channels for flow-induced molecular communication, IEEE Trans. Signal Process. 61 (2013) 5000–5013.

[37] A.O. Bicen, I.F. Akyildiz, End-to-end propagation noise and memory analysis for molecular communication over microfluidic channels, IEEE Trans. Commun. 62 (2014) 2432–2443.

[38] D.A. Neamen, Fundamentals of the Metal–Oxide–Semiconductor Field-Effect Transistor, McGraw-Hill, 2012.

[39] T. Bakhshi, S. Shahid, Securing internet of bio-nano things: ml-enabled parameter profiling of bio-cyber interfaces, in: 2019 22nd International Multitopic Conference (INMIC), IEEE, 2019, pp. 1–8.

[40] C. Camara, P. Peris-Lopez, J.E. Tapiador, Security and privacy issues in implantable medical devices: a comprehensive survey, J. Biomed. Inf. 55 (2015) 272–289.

[41] G. Sharma, S. Bala, A.K. Verma, Security frameworks for wireless sensor networks-review, Procedia Technol. 6 (2012) 978–987.

[42] M. Usman, M.R. Asghar, I.S. Ansari, M. Qaraqe, Security in wireless body area networks: from in-body to off-body communications, IEEE Access 6 (2018) 58064–58074.

[43] J. Tang, S. Alelyani, H. Liu, Feature Selection for Classification: A Review. Data Classification: Algorithms and Applications, 2014, p. 37.

[44] M. Kuscu, O.B. Akan, On the capacity of diffusion-based molecular communications with sinw fet-based receiver, in: 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE, 2016, pp. 3043–3047.

[45] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, A. Razaque, Cascaded hybrid intrusion detection model based on som and rbf neural networks, Concurrency Comput. Pract. Ex. 32 (2020), e5233.

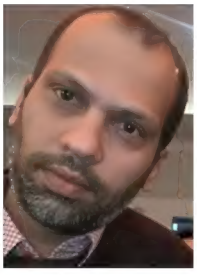
[46] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, A. Razaque, Deep recurrent neural network for iot intrusion detection system, Simulat. Model. Pract. Theor. 101 (2020) 102031.

[47] M.J. Kang, J.W. Kang, Intrusion detection system using deep neural network for in-vehicle network security, PloS One 11 (2016), e0155781.

[48] A. Shenfield, D. Day, A. Ayesh, Intelligent intrusion detection systems using artificial neural networks, ICT Express 4 (2018) 95–99.

[49] Q. Bai, Analysis of particle swarm optimization algorithm, Comput. Inf. Sci. 3 (2010) 180.
[50] A.P. Engelbrecht, Computational Intelligence: an Introduction, John Wiley & Sons, 2007.
[51] A.S. Saljoughi, M. Mehrvarz, H. Mirvaziri, Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms, Emerg. Sci. J. 1 (2017) 179–191.
[52] V.G. Gudise, G.K. Venayagamoorthy, Comparison of particle swarm optimization and backpropagation as training algorithms for neural networks, in: Proceedings of the 2003 IEEE Swarm Intelligence Symposium. SIS'03 (Cat. No. 03EX706), IEEE, 2003, pp. 110–117.

Sidra Zafar is a Ph.D. scholar at Lahore College for Women University (LCWU), Lahore, Pakistan. She received her MS (Computer Science) from LCWU in 2012. She did her BS (Software Engineering) from International Islamic University Islamabad, Pakistan. She has presented her work at the International Conference. Her research interests include the Internet of Nano Things, Nano Communication Network, Security in Nanonetworks, Access Control.



Dr. Mohsin Nazir is the in charge at Lahore College for Women University Pakistan in the Dept. of Software Engineering & adjunct faculty member in various institutes. He earned his PhD & MS degree from Asian Institute of Technology Thailand in Information & Communications Technologies. His BS degree in computer sciences is from National University of Computer and Emerging Sciences, Islamabad, Pakistan. Since 2003, he has been associated with Lahore College for Women University Pakistan, where he was involved in Research, Development and teaching in the ICT Department. He has numerous publications to his credit & is an editorial board member of many research journals. He has organized and participated in many national and international conferences. He also worked as Research Scientist in the Center for Wireless Communications at University of Oulu, Finland. His area of research involves application of Information & Communications Technologies for real time applications.

Dr. Aneeqa Sabah is currently working as an Assistant professor in physics department LCWU. She has been Awarded for Overseas Scholarship for PhD degree in the field of Nanotechnology by HEC (Higher education commission), Pakistan. It was a successful project. She has been supervising the several projects on BS, MS, and PhD level, based on nano fabrication, nano films and membranes, quantum dots, hybrid materials, spectroscopy, composites, and metal doped sensing. She has published many research papers in high impact factor journals, journal of physical chemistry and ACS, and involved in participating and organizing seminar and conferences in respective departments. Her expertise is nano synthesis, self-assembly and organization, colloids, one dimensional nano materials, green chemistry, and quantum dots.

Dr. Anca Jurcut is an Assistant Professor in the School of Computer Science, University College Dublin (UCD), Ireland, since 2015. She received a BSc in Computer Science and Mathematics from West University of Timisoara, Romania in 2007 and a PhD in Security Engineering from the University of Limerick (UL), Ireland in 2013 funded by the Irish Research Council for Science Engineering and Technology. She worked as a postdoctoral researcher at UL as a member of the Data Communication Security Laboratory and as a Software Engineer in IBM in Dublin, Ireland in the area of data security and formal verification. Dr. Jurcut research interests include Security Protocols Design and Analysis, Automated Techniques for Formal Verification, Network Security, Attack Detection and Prevention Techniques, Security for the Internet of Things, and Applications of Blockchain for Security and Privacy. Dr. Jurcut has several key contributions in research focusing on detection and prevention techniques of attacks over networks, the design and analysis of security protocols, automated techniques for formal verification, and security for mobile edge computing (MEC). More Info: https://people.ucd.ie/anca.jurcut.